UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,443	04/30/2001	Gregory G. Rose	QCPA454B1C1	5374

23696 7590 01/04/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,443	ROSE, GREGORY G.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) ~~*1, 3 and 4*~~ 1-4 is/are rejected.

7)☒ ~~Claim(s) 2 is/are objected to~~. No claims are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 02 July 2004. Claim 1 has been amended. No claims have been added or canceled. Claims 1-4 are currently pending in the present application.

Drawings

2. The objection to the drawings is withdrawn in view of the amendment to Figure 2.

Claim Rejections - 35 USC § 112

3. The rejection of claims 1-4 under 35 U.S.C. 112, second paragraph, as being indefinite is withdrawn in view of the amendments to the claims.

Response to Arguments

4. Applicant's arguments with respect to claims 1-4 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi, US Patent 5206824, in view of Bianco et al, US Patent 5365588, and Falk, US Patent 5249144.

In reference to Claim 1, Arazi discloses a method for generating a non-linear output from a linear feedback shift register that includes shifting bits through the LFSR and performing modular multiplications on the bits (column 4, lines 49-53). However, Arazi does not disclose performing a non-linear operation on a selected portion of the shifted bits, nor does Arazi explicitly disclose implementing the modular multiplications using look-up tables.

Bianco discloses an encryption method that includes an LFSR, in which bits shifted by the LFSR are used as the inputs to non-linear functions (column 3, lines 23-28; see also Figure 1 where Working Register 70 is an LFSR and Output Functions 80A-80N are non-linear). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the non-linear functions in the method of Arazi, in order to make the encryption algorithm more robust and resistant to cryptanalysis (see Bianco, column 1, lines 37-39).

Bianco further discloses that the non-linear functions can be implemented using ROM as look-up tables (column 5, lines 3-24); however, Bianco does not explicitly disclose using the look-up tables to implement modular multiplication. Falk discloses an arithmetic logic unit (ALU) in which a look-up table can be used to perform modular arithmetic functions (column 4, lines 26-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Arazi in view of Bianco by implementing the modular multiplication using look-up tables, in order to allow the combination of functions to perform modular arithmetic functions (see Falk, column 1, lines 53-60).

In reference to Claim 4, Bianco further discloses initializing the LFSR by adding a key to an element of the LFSR (column 4, lines 33-35, where a random sequence is loaded into the working register) and adding a second key to the LFSR for each frame of data (column 4, lines 8-19, where the content of the key register is combined with the output feedback before being input to each cell of the working register).

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi in view of Bianco and Falk as applied to claim 1 above, and further in view of Rose et al, US Patent 6560338.

The applied reference has a common inventor with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in

the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). For applications filed on or after November 29, 1999, this rejection might also be overcome by showing that the subject matter of the reference and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. See MPEP § 706.02(l)(1) and § 706.02(l)(2).

Arazi in view of Bianco and Falk disclose everything as applied above to Claim 1. Bianco further discloses using functions defined as non-linear over a Galois Field (column 6, lines 31-36). However, neither Arazi, Bianco, nor Falk explicitly discloses a non-linear operation defined as $V_n = (S_n + S_{n+5}) \times (S_{n+2} + S_{n+12})$ defined over $GF(2^8)$. Rose discloses a non-linear function defined as $V_n = (S_n + S_{n+5}) \times (S_{n+2} + S_{n+12})$ (column 11, equation 5) that is defined over $GF(2^8)$ and can be applied to the output of an LFSR to generate a stream cipher (column 11, line 1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as disclosed by Arazi as modified above by including the use of the non-linear function defined above, in order to remove linearity in the output of an LFSR (see Rose,

column 3, lines 6-19) and in order to optimize security and efficiency (see Rose, column 3, lines 50-53).

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi in view of Bianco and Falk as applied to claim 1 above, and further in view of Bardell, Jr., US Patent 4959832.

Arazi in view of Bianco and Falk disclose everything as applied above to Claim 1; however, they do not explicitly disclose the use of a stuttering operation. Bardell discloses that stuttering can be used on the output of an LFSR (column 7, lines 43-60, where decimation reads on stuttering). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as disclosed by Arazi as modified above by including the use of a stuttering operation, in order to produce the maximum number of distinct output patterns of the LFSR (see Bardell, column 7, lines 31-33).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Davida, US Patent 4202051, discloses a method for enciphering and deciphering that includes using the output of an LFSR as the input of a non-linear finite state machine.

b. Lee et al, US Patent 4852023, discloses non-linear random generators that include an LFSR and a non-linear function.

c. Finkelstein, US Patent 5060265, discloses a method for adding non-linearity to the output of an LFSR to protect against cryptanalysis.

d. Shimada, US Patent 5566099, discloses a random number generator using LFSRs and a non-linear function circuit.

e. Vigoda, US Patent 6724805, discloses a system that includes an LFSR feeding a non-linear element.

f. Driscoll, US Patent 6763363, discloses an LFSR that can include non-linear operations on the output and clock control of the output.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell
Andrew Caldwell